

Телефонное мошенничество.

Какие схемы используют мошенники с использованием номера телефона

На сегодняшний день мошенничество, при котором злоумышленники представляются представителями операторов сотовой связи или сотрудниками других различных структур, является одним из распространённых видов телефонного мошенничества. Номер мобильного телефона в наше время – это ключ к банковским приложениям, электронным госуслугам, личной информации. Мошенники это понимают, поэтому все чаще представляются сотрудниками компаний-операторов сотовой связи с целью завладеть деньгами или личными данными доверчивых людей. Особое внимание злоумышленников привлекают наиболее уязвимые категории граждан такие как дети, подростки и пожилые люди.

О некоторых схемах мошенничества и о том, как от них защититься рассмотрим в данной статье.

Схемы телефонного мошенничества

Схема № 1: «Продление или перерегистрация договора обслуживания»

Эта схема заключается в том, что вам поступает звонок от сотрудника оператора сотовой связи, который начинает убеждать вас в том, что обслуживание абонента скоро заканчивается и связь будет отключена, потом объясняют вам, что для того чтобы этого не произошло, необходимо совершить одно из предлагаемых действий, таких как: передать паспортные данные, продиктовать коды из СМС, зайти в Госуслуги или в банковское приложение. С помощью полученных данных и СМС кодов мошенники получают персональные данные для кражи денег с банковских счетов, оформления кредита и других преступных действий.

Как себя защитить! После получения просьбы о предоставлении смс – кода или передачи каких либо данных, лучше прекратить беседу с мошенником.

Настоящий договор мобильной связи бессрочен и не подразумевает ежегодного обновления. После этого желательно самостоятельно связаться с оператором сотовой связи по известным номерам, размещенным на официальном ресурсе, чтобы подтвердить информацию.

Оператор сотовой связи может в одностороннем порядке приостановить обслуживание абонента только в том случае, если абонент нарушает требования договора, например, не оплачивает услуги связи. И даже в этом случае оператор сотовой связи обязан уведомить абонента о приостановлении оказания услуг связи до устранения нарушения и намерении расторгнуть договор в случае неустранения нарушения через 6 месяцев со дня получения абонентом такого уведомления.

Схема № 2: «Блокировка счета»

При применении этой схемы, мошенники отправляют на Ваш номер телефона сообщение следующего содержания: «Ваш счёт временно заблокирован. Для разблокировки перезвоните по номеру XXXX». Часто такие сообщения присылают от имени оператора сотовой связи.

Однако, не стоит перезванивать по номеру указанному в сообщении, это может привести к списанию денежных средств с вашего счета.

Конечно, номер абонента может быть заблокирован оператором сотовой связи, и об этом может прийти сообщение от реального оператора. Но разблокировка номера не производится по звонку оператору сотовой связи. Поэтому наличие блокировки всегда можно отследить в личном кабинете абонента на сайте или в приложении оператора сотовой связи.

Схема № 3: «От вас поступила заявка на смену мобильного оператора»

По этой схеме на ваш номер телефона поступает звонок или сообщение от сотрудников оператора связи, который просит подтвердить или изменить переход к другому оператору с помощью смс - кода, так же могут предложить «помощь» со сменой пароля в личном кабинете, если вдруг вы сказали, что не оставляли такую заявку.

На самом же деле, действительно можно поменять онлайн мобильного оператора с сохранением номера, но для этого не нужно называть смс – коды.

Если вам поступил такой звонок в котором говорят, что от вас поступила заявка на перенос номера, лучше завершите разговор, и перезвоните операторам сотовой связи по официальным номерам и уточните, правда ли это.

Общие рекомендации по защите своих данных

- **Не передавайте никому коды из SMS.** Даже если вам звонят и утверждают, что являются сотрудниками оператора связи, банка, полиции, государственного ведомства. Никогда никому не сообщайте одноразовые коды, полученные через SMS или другие каналы. Такие данные спрашивают по телефону только мошенники.
- **Не предоставляйте личную информацию.** Не сообщайте посторонним лицам свою фамилию, имя, адрес проживания. Тем более держите при себе номера паспорта или банковской карты. Личные данные могут использоваться против вас.
- **Прекращайте разговор.** Если почувствовали малейшее подозрение, немедленно завершайте разговор. Любые настойчивые и срочные просьбы передать информацию — явный признак мошеннической схемы.
- **Удаляйте подозрительные сообщения.** Если вам приходят сомнительные SMS, e-mail или сообщения в мессенджерах, не отвечайте на них. Не переходите по ссылкам и не звоните на предложенные номера телефонов. Лучше всего удалить эти сообщения и заблокировать отправителя.
- **Перепроверьте информацию.** Если возникли сомнения относительно звонка по услугам связи, свяжитесь с контактными центром вашего оператора, найдите официальный аккаунт оператора в соцсети и напишите туда.

*Информация подготовлена специалистами
консультационного центра по защите прав потребителей
«ФБУЗ «Центр гигиены и эпидемиологии в Иркутской области»
с использованием интернет – ресурсов:*

<https://media.mts.ru>,

<https://www.garant.ru/article/1814213>

<https://t-j.ru/list>

НАШИ КОНТАКТЫ:

г. Иркутск, ул. Трилиссера 51, каб. 113

тел.: 8 (395-2) 22-23-88,

г. Иркутск, Пушкина 8, каб. 101

тел.: 8 (395-2) 63-66-22,

e-mail: zpp@sesoirkutsk.ru